538,685

(54) Title: IMPROVED MONEY ITEM ACCEPTOR
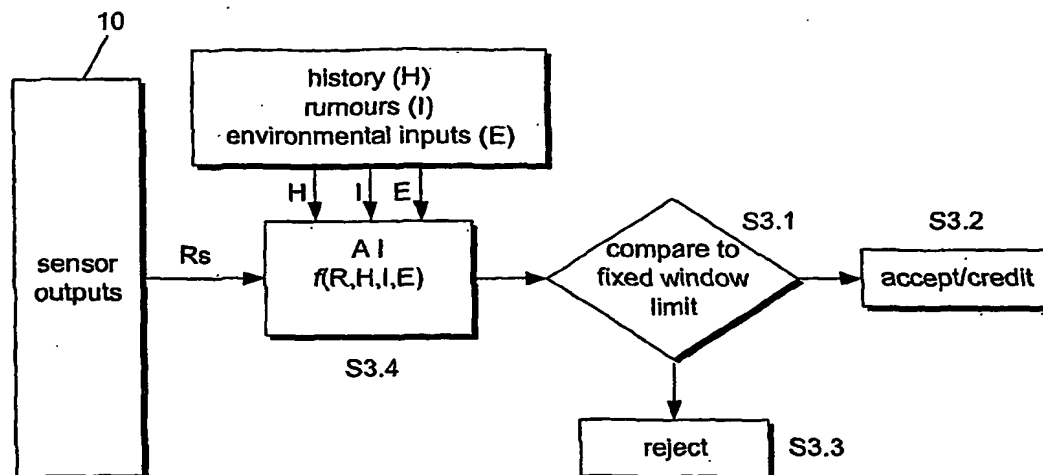
(57) Abstract: An acceptor for money items, comprises sensor circuitry (S1-S4) to provide individual money items signals (Rs) depending on items of money under test, and a processor configuration (11) to develop for each of the money items under test, a transformed money item signal (Tnew) as a function of the value of the money item signal and at least one variable parameter (A) that is a function of a fraud criterion such as history data (AVG Dn & MAX Dn) relating to the values of the money item signals for previously tested money items, to make a comparison of the values of the transformed money item signals (Tnew) with a fixed window limit value (W2, L3) and to accept each money item if it falls within the window limit.

WO 2004/063996 A1

Improved Money Item Acceptor

Description

Field of the invention

5   This invention relates to an acceptor for money items such as coins and

banknotes and has particular but not exclusive application to a multi-

denomination acceptor.

Background of the invention

10   Coin and banknote acceptors are well known. One example of a coin acceptor is

described in our GB-A-2 169 429. The acceptor includes a coin rundown path

along which coins pass through a coin sensing station at which sensor coils

perform a series of inductive tests on the coins in order to develop coin

parameter signals which are indicative of the material and metallic content of the

15   coin under test. The coin parameter signals are digitised and compared with

stored coin data by means of a microcontroller to determine the acceptability or

otherwise of the test coin. If the coin is found to be acceptable, the

microcontroller operates an accept gate so that the coin is directed to an accept

path. Otherwise, the accept gate remains inoperative and the coin is directed to

20   a reject path.

In banknote validators, sensors detect characteristics of the banknote. For

example, optical detectors can be used to detect the geometrical size of the

banknote, its spectral response to a light source in transmission or reflection, or

25   the presence of magnetic printing ink can be detected with an appropriate

sensor. The parameter signals thus developed are digitised and compared with

stored values in a similar way to the previously described prior art coin acceptor.

The acceptability of the banknote is determined on the basis of the results of the

comparison.

30

When a number of coins or banknotes of the same denomination are passed

through an acceptor, successive values of coin or banknote parameter data are

thus developed. When the distribution of the values of these signals is plotted as a graph, the result is a bell curve, with a central peak and tails on opposite sides. The shape of the graph may typically although not necessarily be Gaussian.

5   The distribution illustrates that for a money item, such as a coin or banknote of a particular denomination, the most probable value of the corresponding parameter signal lies at the peak of the bell curve, with a decreasing probability to either side. In prior coin and banknote acceptors data is stored in a memory, corresponding to acceptable ranges of parameter signal for a particular

10   denomination. The acceptor compares the value for a coin or banknote under test with the stored data to determine authenticity. The data may define windows in terms of upper and lower limit values, or as a mean value and a standard deviation, such that the window comprises a predetermined number of standard deviations about the mean. By making the stored windows narrow, an

15   increased discrimination is provided between true money items and frauds. However, if the windows are made too narrow, the rejection rate of true money items increases, disadvantageously. The width of the windows is thus selected as a compromise between these two factors. Attempts to defraud coin or banknote acceptors typically involve the manufacture of facsimile coins or banknotes,

20   which cause the acceptor to produce parameter signals which lie within the stored acceptance windows. Hitherto, coin acceptors have been provided with relatively wide and narrow window widths so that the operator can manually select the wide window width for normal operation and the narrow window width if frauds are being presented for validation. An example is described in

25   Japanese unexamined patent application no Hei 2-197985.

A number of different approaches have been proposed to vary the window width dynamically to improve discrimination between true and false coins. In US-A-5 355 989, a coin acceptor is described which switches automatically from a first

30   normal acceptance window for a true coin, to a second narrower window when a coin parameter signal produced by testing a coin falls in a region of the normal window for the true coin corresponding to a low acceptance probability region.

for the coin concerned. A group of fraudulent coins may all have similar characteristics and they may cause the acceptor to produce parameter signals which lie within the normal window, but the parameter signals consistently have a value which is not centred on the high probability peak region of the window

5 associated with the true coin and instead are centred on the lower probability tail regions of the bell curve distribution within the normal window. When the parameter signal falls within this low probability region, the second narrower window is then used for the next tested coin. If the next coin has a parameter falling in the narrower window it is a true coin, but if not, it is a fraud that

10 should be rejected. This approach seeks to prevent frauds carried out by the use of coins of a particular low value denomination, from a foreign currency set, with characteristics that correspond but are not exactly the same as a high value coin of the currency set that the acceptor is designed to accept. It will be understood that the foreign denomination coins exhibit their own generally

15 Gaussian distribution of parameter signals, and if the low probability or tail region of this distribution partially overlaps a corresponding region of the distribution for the true coin that the acceptor is designed to accept, then the low value foreign coins will sometimes be accepted as true coins.

20 Another approach is described in EP-A-0480736, in which the acceptance window is based on the value of a coin parameter for previous acceptable coins, as long as the previous coin parameter values do not deviate significantly from one another. This enables the coin acceptor to self-tune the window to take account of changes in operating parameters such as temperature and other long

25 term drifts. A danger with this approach is that the coin acceptor can be taught to modify its window so as to accept frauds by using fraudulent coins similar to true coins. To overcome this problem, a so-called near miss area is defined and if a coin parameter signal from a coin under test falls in this area, this indicates the risk of a fraud and the window is shifted away from the area to prevent the

30 window position being influenced by the potential fraud. However, the position of the near miss area is critical in order to avoid falsely detecting true items as a fraud attack. To this end the near miss area must be a reasonable distance

outside of the true coin population (particularly if the error in positioning the centre of the window is taken into account). This creates a gap were a sufficiently close fraud attempt can still trigger a window shift before it is spotted in the near miss area. It may also be possible to utilise slightly modified.

5   true coins or even a different fraud on the other side of the window to train the window towards the original fraud attempt. The method described in EP-A-0480736 is therefore only of use for relatively poor quality frauds and a more stringent system is needed to counter a stronger fraud attack..

10   Summary of the invention

The present invention provides an alternative approach, which does not involve the complication of having to control the window width.

According to the invention there is provided a method of accepting of money
15   items, comprising: generating individual money items signals with a value that is a function of respective items of money under test, developing for each of the money items under test, a transformed money item signal as a function of the value of the money item signal and at least one variable parameter that is a function of the acceptability criterion for the money item under test, making a
20   comparison of the values of the transformed money item signals with a window limit value, and accepting each money item in dependence upon said comparison.

The variable parameter may be a function of history data relating to the values of the money item signals for previously tested money items.

25
The transformed money item signal may developed by transforming the money item signal according to the outcome of a rules based expert system that determines the occurrence of the acceptability criterion. More particularly, the transformed money item signal may be developed by scaling the money item signal for a money item under
30   test in accordance with an amplification factor determined in dependence on the outcome of a comparison of data based on previously tested money items with one or

more rules. Different amplification factors may be used, depending on the outcome of the comparisons for the rules.

An average of data corresponding to the money item signals for previously tested money items may be compared with a first limit value lying within a window delimited by said window limit, and if the average is not within said first limit, the money item signal for a money item under test may be scaled in accordance with the amplification factor.

Also, a maximum value of data corresponding to the values of money item signals for previously tested money items may be compared with a second limit value lying within a window delimited by said window limit, and if said maximum value is not within said second limit, the money item signal for a money item under test may be scaled in accordance with the amplification factor.

The window limit may delimit an acceptance window as deviation relative to a window mean, and the value of a money item signal for a money item may be adjusted relative to the window mean, mode or median, whereby to produce an error signal and the transformed money item signal may be developed from the error signal.

The invention also includes an acceptor for money items, comprising: sensor circuitry to provide individual money items signals of a value as a function of respective items of money under test, and a processor configuration to develop for each of the money items under test, a transformed money item signal as a function of the value of the money item signal and at least one variable parameter that is a function of a acceptability criterion for the money item under test, to make a comparison of the values of the transformed money item signals with a window limit value, and to accept each money item in dependence upon said comparison.

Brief description of the drawings

In order that the invention may be more fully understood an embodiment thereof will now be described by way of example with reference to the accompanying drawings in which:

5   Figure 1 is a schematic block diagram of a coin acceptor in accordance with the invention;

Figure 2 is a schematic block diagram of the circuits of the acceptor shown in Figure 1;

Figure 3 is a schematic block diagram of a coin acceptance process carried out by

10   the microcontroller shown in Figure 1;

Figure 4 illustrates the configuration of an acceptance window with a fixed window limit;

Figure 5 is a schematic diagram of data derived from successive coins under test in relation to the fixed window data and other limits; and

15   Figure 6 is a flow diagram of a coin acceptance process in accordance with the invention.

Detailed description

Overview of coin acceptor

20   Figure 1 illustrates the general configuration of an acceptor according to the invention, for use with coins. The coin acceptor is capable of validating a number of coins of different denominations, including bimet coins, for example the euro coin set and the UK coin set including the bimet £2.00 coin. The acceptor includes a body 1 with a coin run-down path 2 along which coins under

25   test pass edgewise from an inlet 3 through a coin sensing station 4 and then fall towards a gate 5. A test is performed on each coin as it passes through the sensing station 4. If the outcome of the test indicates the presence of a true coin, the gate 5 is opened so that the coin can pass to an accept path 6, but otherwise the gate remains closed and the coin is deflected to a reject path 7. The path

30   through the acceptor for a coin 8 is shown schematically by dotted line 9.

The coin sensing station 4 includes four coin sensing coil units S1, S2, S3 and S4, which are energised in order to produce an inductive coupling with the coin. Also, a coil unit PS is provided in the accept path 6, downstream of the gate 5, to act as a credit sensor in order to detect whether a coin that was determined to be

5   acceptable, has in fact passed into the accept path 6.

The coils are energised at different frequencies by a drive and interface circuit 10 shown schematically in Figure 2. Eddy currents are induced in the coin under test by the coil units. The different inductive couplings between the four coils

10   and the coin characterise the coin substantially uniquely. The drive and interface circuit 10 produces corresponding digital coin parameter data signals R_S, namely R_1, R_2, R_3, R_4, as a function of the different inductive couplings between the coin and the coil units S1, S2, S3 and S4. A corresponding signal is produced for the coil unit PS. The coils S have a small diameter in relation to

15   the diameter of coins under test in order to detect the inductive characteristics of individual chordal regions of the coin.

In order to determine coin authenticity, the coin parameter signals produced by a coin under test are fed to a microcontroller 11, which is coupled to a memory 12.

20   The microcontroller 11 processes the coin parameter signals R_1 .... R_4 derived from the coin under test and compares the outcome with corresponding stored values held in the memory 12. The stored values are held in terms of windows having upper and lower value limits. Thus, if the processed data falls within the corresponding windows associated with a true coin of a particular denomination,

25   the coin is indicated to be acceptable, but otherwise is rejected. If acceptable, a signal is provided on line 13 to a drive circuit 14 which operates the gate 5 shown in Figure 1 so as to allow the coin to pass to the accept path 6. Otherwise, the gate 5 is not opened and the coin passes to reject path 7. The coin acceptance process performed by the microcontroller 11 may be modified

30   or updated in response to an external input received on line 16.

The microcontroller 11 compares the processed data with a number of different sets of operating window data from the memory 12, appropriate for coins of different denominations so that the coin acceptor can accept or reject more than one coin of a particular currency set. If the coin is accepted, its passage along the

5   accept path 6 is detected by the post acceptance credit sensor coil unit PS, and the unit 10 passes corresponding data to the microcontroller 11, which in turn provides an output on line 15 that indicates the amount of monetary credit attributed to the accepted coin.

10   The sensor coil units S each include one or more inductor coils connected in an individual oscillatory circuit and the coil drive and interface circuit 10 includes a multiplexer to scan outputs from the coil units sequentially, so as to provide data to the microcontroller 11. Each circuit typically oscillates at a frequency in a range of 50-150 kHz and the circuit components are selected so that each sensor

15   coil S1-S4 has a different natural resonant frequency in order to avoid cross coupling between them.

As the coin passes the sensor coil unit S1, its impedance is altered by the presence of the coin over a period of ~100 milliseconds. As a result, the

20   amplitude of the oscillations through the coil is modified over the period that the coin passes and also the oscillation frequency is altered. The variation in amplitude and frequency resulting from the modulation produced by the coin is used to produce the coin parameter signals R_1.... R_4 representative of characteristics of the coin.

25

Coin acceptance process
Figure 3 is a schematic illustration of the process carried out by the microcontroller 11. The process will be described in relation to one of the coin parameter signals R_S in order to simplify the description and it will be

30   understood that a corresponding process will be carried out for each of the coin parameter signals individually. As shown in Figure 3, coin parameter signal R_S is derived from the coin interface and drive circuitry 10 shown in Figure 2. The

signal R_S is converted into a digital signal with a numerical value that corresponds to the coin that gave rise to the signal. The digital conversion may be carried out by the micro controller 11 or within the coin drive and interface circuitry 10 itself. The value of coin parameter signal R_S is compared with a

5 fixed window limit in step S3.1, the window limit being stored in the memory 12. A coin acceptance or rejection signal is produced depending on the outcome of the comparison, as shown at steps S3.2 and S3.3.

Artificial intelligence (AI) is utilised to transform at step S3.4 the value of the

10 coin parameter signal R_S prior to the comparison with the fixed window limit at step S3.3. The AI functionality transforms the coin parameter signal to take account of a number of factors, more particularly, the history of previous coins accepted or rejected, rumours such as indications from adjacent coin acceptors that fraudulent coins are being used in the vicinity and environmental inputs

15 such as changes in temperature. For example, the coin parameter signals may be transformed as described in our EP-A-0399694 to take account of temperature changes or the presence of metal objects in the vicinity of the sensor coils, prior to comparison with the fixed window limit.

20 In this example, the AI functionality comprises a rules based expert system as will now be explained in more detail.

Figure 4 illustrates an example of the fixed window used for the comparison process of step S3.1. The window is stored in terms of a mean value M

25 corresponding to the average value of the coin parameter signal for a coin of a particular denomination. In order to accommodate coins which deviate from the mean, upper and lower fixed window limits W1 and W2 are provided around the mean and may be stored in terms of a deviation relative to the mean M. In the example of Figure 4 the upper and lower window limits W1, W2 are ±7 relative

30 to the mean M but of course other values can be used, which need not be symmetrically disposed about the mean. By providing a window, coins which deviate slightly from the mean will also be accepted. It will be appreciated that if

the window width (W2 - W1) is made too wide, there is an increased risk of fraudulent coins being accepted whereas if the window width is made too narrow, there is a risk that a significant number of true coins will be rejected. The window width needs to be a compromise between these two considerations.

5

Hitherto it has been proposed to change the window when previous coin readings indicate that there is a risk that a fraudulent coin is being presented to the coin acceptor. The following example of the present invention provides an alternative, improved approach using AI in the form of a rules based expert

10 system. The positive going region of the window from the mean value M to the fixed window limit W2 will be considered, namely region A in Figure 4. It will be understood that similar considerations apply to the negative going region from mean value M to window limit W1, which will not be explained in detail in order to simplify the description.

15

Referring to Figure 5, the data derived from the latest or new value of the coin parameter signal R_S is shown together with N previous values for previously tested coins of the same denomination $H1_S....HN_S$. The value of the coin parameter signal for each of the tested coins is shown as a black dot and the coin

20 parameter value has been re-valued relative to the mean M for the fixed window. More particularly, the microcontroller 11 adjusts the values of the coin parameter signals R_S, $H1_S$ etc so as to produce corresponding adjusted data D for use in the rules based system. For example, considering the coin parameter R_S for the coin currently under test, this gives rise to data D_{new} where

25 $$D_{new} = R_S - M$$
In this example,
$$D_{new} = 3$$
Corresponding adjusted historic data $D_1....D_N$ are also derived corresponding to the historic coin parameter signals $H1_S....HN_S$.

30 In this example, $D_1 = 4$ and $D_N = 9$.

The microcontroller 11 is configured to store a predetermined number of previous values of the data D_N for previously tested coins of the same denomination and to keep a running average of them. For example, the last 10 values of D_N may be stored and a running average $AVGD_N$ is computed. Also,

5   the maximum value Max D_n is determined from the stored data D_n on a running basis. The values of Max D_n and $AVGD_N$ are used as history data in the coin acceptance process.

Referring again to Figure 4, when a number of true coins are tested, the

10   corresponding value of $AVGD_N$ should lie close to the mean M. If the average value lies significantly away from the mean, this indicates there is a risk that the validator is under attack by fraudster using false coins. Also, if the value of Max D_n lies more towards the window limit W2 than the mean M, this indicates an increased risk that a fraud attempt is being made.

15

Figure 6 illustrates how the history data is used in the transformation of step S3.4 and the subsequent comparison of the transformed data, with the fixed window limit of step S3.1. Referring to Figure 6 in detail, the validation process starts at step S6.0 and at step S6.1, an "under attack" flag UA is set to the value

20   "false". Similarly, an amplification factor A is initially set to a value of unity and a transformed data parameter T_{new} is initialised to zero.

Then, at step S6.2 the value of $AVGD_N$ is compared with an acceptability criterion defined by a limit value L1 shown in Figure 5. Thus, if the average

25   value of D_n for the last 10 coins under test deviates significantly from the mean M, beyond the limit L1, then there is a risk that the coin acceptor is under attack by a fraudster and the flag UA is set to "true" at step S6.3. Also, the amplification factor A is set to a value >1. In this example, the amplification factor is set to a value of 3 for use subsequently in the transformation process to

30   be described hereinafter.

At step S6.4, the previously computed value of Max D_n is compared with an acceptability criterion defined by a guard limit L2, the value of which is shown in Figure 5. If Max D_n exceeds this limit value, this indicates that one of the previously tested coins has a value of D close to the fixed window limit W2, signifying the risk of a fraud amongst recently detected coins. In this case, the flag UA is set to "true" at step S6.5, indicating that the coin acceptor is under attack by a fraudster. Also, the amplification factor A is set to a value >1 e.g. 4.

Then, at step S6.6, the condition of the flag UA is tested to determine if the acceptor is under attack by a fraudster. If there is no fraud attack, the value of the transformed data parameter T_{new} is set to be the same value as D_{new} corresponding to the coin under test. The value of T_{new} is then compared with a limit value L3 at step S6.9. The limit value L3 corresponds to the fixed window limit W2 shown in Figure 5. Thus, if the value of T_{new} is less than L3, the data corresponds to an acceptable value of D_{new} and hence an acceptable value of R_S for the coin under test.

Conversely, if the T_{new} exceeds the fixed window limit L3 then the coin should be rejected as shown at step S6.11.

In the event that the test of step S6.6 indicates the validator to be under attack, the value of D_{new} for the coin under test is transformed using the amplification factor set at step S6.3 or S6.5. The transformation is carried at step S6.8 so that the parameter T_{new} adopts a value of $D_{new}*A$. The transformed or amplified value is then compared with the fixed window limited L3 at step S6.9 as previously described. Thus, when the coin acceptor is under attack by a fraudster, a more stringent test is applied to the coin data D. It will be understood that because of the amplification factor, the actual value D_{new} for the coin under test needs to be much closer to the value of the mean M for the window in order to be less than the fixed limit L3 as compared with the situation where the validator is not under attack and the amplification factor A is not applied.

Thus, in accordance with the invention, a more stringent test is applied when the acceptor is under fraud attack and in accordance with the invention, a fixed window limit L3 is utilised so that there is no need to change the window

5   position or to switch between different window widths to achieve automatic security protection.

Many modifications and variations fall within the scope of the invention. For example, in certain situations, it may be preferable to test the value of $AVGD_N$

10   against the limit value L1 after testing the value of Max D_n against limit L2. Also, the value of the amplification factor is not limited to the values given above and can be altered according to particular circumstances.

In the example described hereinbefore, the acceptability criteria corresponding to

15   the limits L1 and L2 constitute fraud criteria for determining when a fraud attack occurs, and one or more amplification factors greater than one (A>1) are used in order to provide enhanced discrimination against frauds. However, when a run of acceptable coins has occurred, it may be advantageous to use an amplification factor 0>A<1 to increase the likelihood of coins being accepted when the risk of

20   occurrence of a fraud is relatively low.

Also, the data used to produce the running average $AVGD_N$ and also Max D_n may be time dependent, so that coin parameter signals from coins tested more than a particular time ago will be ignored for the purposes of determining

25    $AVGD_N$ and Max D_n.

Furthermore, the rules based expert system can include additional or alternative rules for determining the criteria under which the amplification factor A is applied in response to a fraudster. Also, different rules can be used that do not

30   use comparisons between scaled signals and thresholds. Furthermore, transformations other than a simple amplification may be used, such as non-linear transformations, offsets and combinations thereof. For example, as shown

schematically in Figure 3, rumours (I) from adjacent coin acceptors that a
fraudster is in the vicinity of a group of machines may be used to set the value of
the amplification factor A or other transformation for a period of time so as to
apply a more stringent test to coins in response to the rumour. The rumour data
5   may be received on input 16 shown in Figure 2. Also, environmental inputs such
as temperature may be applied to impose additional rules based tests to the data
as a function of temperature or time of day, for example in a situation where
frauds are found to happen at particular times e.g. pub closing time. Also,
environmental inputs may be used to shift the window limits W1, W2 long term
10   over time to take account of changes in temperature or other factors.

In the foregoing example, the processing of signals for one of the sensors S is
described and it will be understood that each of sensor output is processed
individually. The processing for one sensor may however take account of the
15   outcome for another sensor and the occurrence of a fraud criterion for one of
the sensors may be used to set an acceptability criterion for the processing of
signals for another of the sensors.

The invention is not limited to the use of an expert, rules based system to
20   perform the AI process shown at step S3.4 in Figure 3. Alternatives include
fuzzy logic, the neural network or a genetic algorithm.

It will be appreciated that the various rules of the rules based system may be
applied individually or collectively on a time basis so that a rule may be applied
25   for a particularly time period and then removed either in response to a coin
acceptance event or in response to external factors

It will also be appreciated that the invention is not restricted to coin validators
but may be used for other money items such as tokens, banknotes, cards and
30   other items having an attributable monetary value.

Claims

1.   A method of accepting of money items, comprising: .

generating individual money items signals with a value that is a function

5   of respective items of money under test,

developing for each of the money items under test, a transformed money item signal as a function of the value of the money item signal and at least one variable parameter that is a function of an acceptability criterion for the money item under test,

10   making a comparison of the values of the transformed money item signals with a window limit value, and

accepting each money item in dependence upon said comparison.

2.   A method according to claim 1 wherein said variable parameter is a

15 function of history data relating to the values of the money item signals for previously tested money items.

3.   A method according to claim 1 or 2 wherein the transformed money item signal is developed by transforming the money item signal according to the

20 outcome of a rules based expert system.

4.   A method according to claim 3 wherein the transformed money item signal is developed by scaling the money item signal for a money item under test in accordance with an amplification factor determined in dependence on the outcome of a comparison of data based on previously tested money items with at

25 least one rule.

5.   A method according to claim 4 including two or more of said rules and including using different amplification factors depending on the outcome of the comparisons for the rules.

30 6.   A method according to claim 4 including comparing an average of data corresponding to the money item signals for previously tested money items with a first limit value lying within a window delimited by said window limit, and if

said average is not within said first limit, scaling the money item signal for a money item under test in accordance with said amplification factor.

7. A method according to claim 4 or 5 including comparing a maximum value of data corresponding to the values of money item signals for previously tested money items with a second limit value lying within a window delimited by said window limit, and if said maximum value is not within said second limit, scaling the money item signal for a money item under test in accordance with said amplification factor.

8. A method according to any preceding claim wherein the window limit has a fixed value.

9. A method according to any preceding claim wherein the window limit delimits a window as deviation relative to a window mean, and including re-valuing the money item signal for a money item relative to the window mean, whereby to produce re-valued money item data and developing the transformed money item signal from said re-valued money item data.

10. A method according to any preceding claim performed in a coin acceptor, and including varying the transformation of the money item signals in dependence on data received from a source externally of the acceptor.

11. A method according to claim 10 wherein the data received from the external source comprises data indicative that of a fraud attack on other acceptors.

12. A method according to any preceding claim wherein the acceptability criterion comprises a fraud criterion corresponding to a fraud attack.

13. A method according to any preceding claim wherein the money items comprise coins or tokens.

14.   An acceptor for money items, comprising:

sensor circuitry to provide individual money items signals of a value as a function of respective items of money under test, and

5   a processor configuration to develop for each of the money items under test, a transformed money item signal as a function of the value of the money item signal and at least one variable parameter that is a function of a acceptability criterion for the money item under test, to make a comparison of the values of the transformed money item signals with a window limit value, and

10   to accept each money item in dependence upon said comparison.

15.   A money item acceptor according to claim 14 wherein said variable parameter is a function of history data relating to the values of the money item signals for previously tested money items.

15

16.   A money item acceptor according to claim 14 or 15 wherein the processor configuration is operable to develop the transformed money item signal by transforming the money item signal according to the outcome of a rule based expert system.

20

17.   A money item acceptor according to claim 16 wherein the processor configuration is operable to develop the transformed money item signal by scaling the money item signal for a money item under test in accordance with an amplification factor determined in dependence on the outcome of a comparison

25   of data based on previously tested money items with at least one rule.

18.   A money item acceptor according to claim 17 including two or more of said rules and wherein the processor configuration is operable to use different amplification factors depending on the outcome of the comparisons for the

30   rules.

19.   A money item acceptor according to claim 17 or 18 wherein the processor configuration is operable to compare an average of data corresponding to the money item signals for previously tested money items with a first limit value lying within a window delimited by said window limit, and if said average is not within said first limit, to scale the money item signal for a money item under test in accordance with said amplification factor.

20.   A money item acceptor according to claim 17 or 18 wherein the processor configuration is operable to compare a maximum value of data corresponding to the values of money item signals for previously tested money items with a second limit value lying within a window delimited by said window limit, and if said maximum value is not within said second limit, to scale the money item signal for a money item under test in accordance with said amplification factor.

21.   A money item acceptor according to any one of claims 14 to 20 wherein the window limit has a fixed value.

22.   A money item acceptor according to any one of claims 14 to 21 wherein the window limit delimits a window as deviation relative to a window mean, and the processor configuration is operable to re-value the value of a money item signal for a money item relative to the window mean, whereby to produce re-valued money item data, and to develop the transformed money item signal from said re-valued money item data.

23.   A money item acceptor according to any one of claims 14 to 23 wherein the processor configuration is operable to control the transformation of the money item signals in dependence on data received from an external source.

24.   A money item acceptor according to claim 23 wherein the data received from the external source comprises data indicative of a fraud attack on other acceptors.

25.   An acceptor according to any one of claim 14 to 24 operable to accept coins or tokens.

5   26.   A multi-denomination acceptor according to any one of claims 14 to 25.
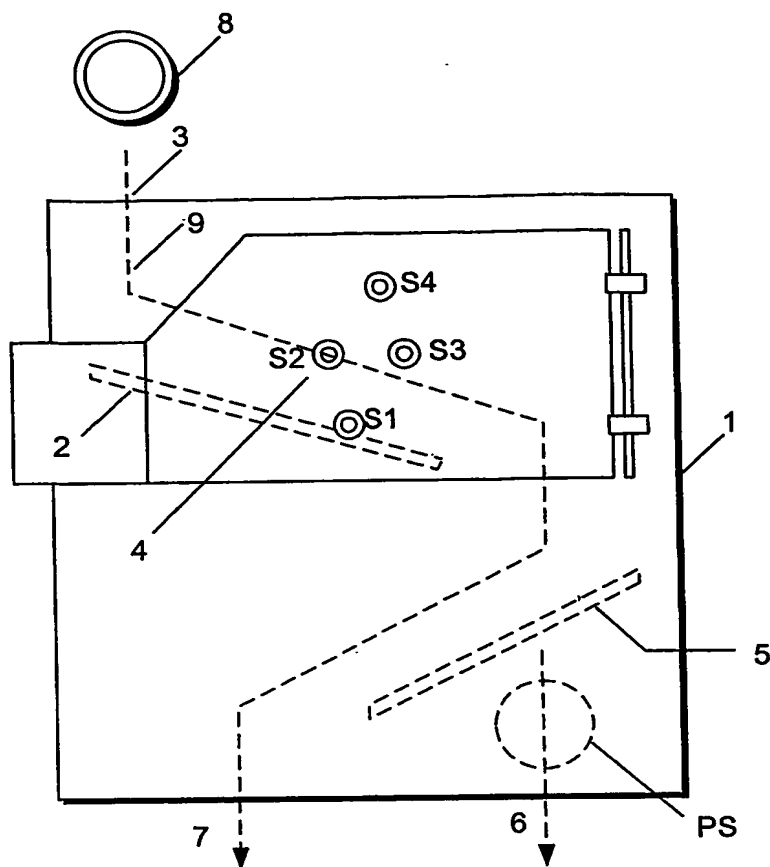
8

3

9

◎S4

S2◎ ◎S3

◎S1

2

4

1

5

PS

7   6

FIG. 1

12

MEMORY

FIG. 2

10

S1

S2

S3

S4

PS

COIL DRIVE.&
INTERFACE

MICROCONTROLLER

11

13

14

GATE
DRIVER

15

16

FIG. 3

FIG. 4

FIG. 5

```
        ┌────────────────────┐
        │  Start Validation  │         S6.0
        └────────────────────┘
                  │
                  ▼
        ┌────────────────────┐
        │ Under attack UA=false│
        │ amplification factor A=1│    S6.1
        │      Tnew=0         │
        └────────────────────┘
                  │
                  ▼
S6.2          ◇ AVG Dn>L1? ◇────────yes──────┐
                  │                            ▼
                  │no                  ┌──────────────┐
                  │                    │   Set A=3    │  S6.3
                  │                    │   UA=true    │
                  │                    └──────────────┘
                  │◄───────────────────────────┘
                  ▼
S6.4          ◇ Max Dn>L2? ◇────────yes──────┐
                  │                            ▼
                  │no                  ┌──────────────┐
FIG. 6            │                    │   Set A=4    │  S6.5
                  │                    │   UA=true    │
                  │                    └──────────────┘
                  │◄───────────────────────────┘
                  ▼
S6.6          ◇    UA?    ◇────────True──────┐
                  │                           │
                  │False                      │
                  ▼                           ▼
S6.7    ┌──────────────┐          ┌──────────────────┐
        │ Tnew=Dnew    │          │  Tnew=Dnew*A     │  S6.8
        └──────────────┘          └──────────────────┘
                  │                           │
                  │◄──────────────────────────┘
                  ▼
S6.9          ◇ Tnew<L3? ◇────────no──────┐
                  │                         │
                  │yes                      │
                  ▼                         ▼
S6.10   ┌──────────────┐          ┌──────────────┐
        │   accept     │          │    reject    │  S6.11
        └──────────────┘          └──────────────┘
```
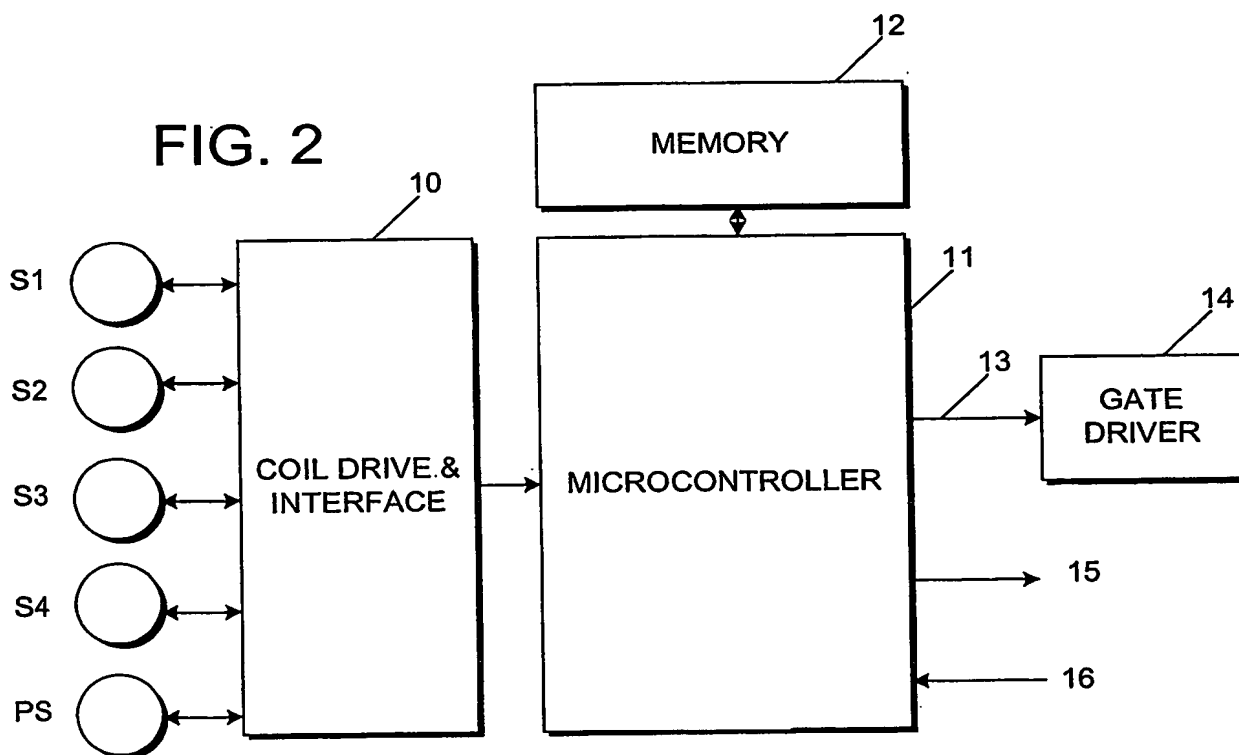
INTERNATIONAL SEARCH REPORT

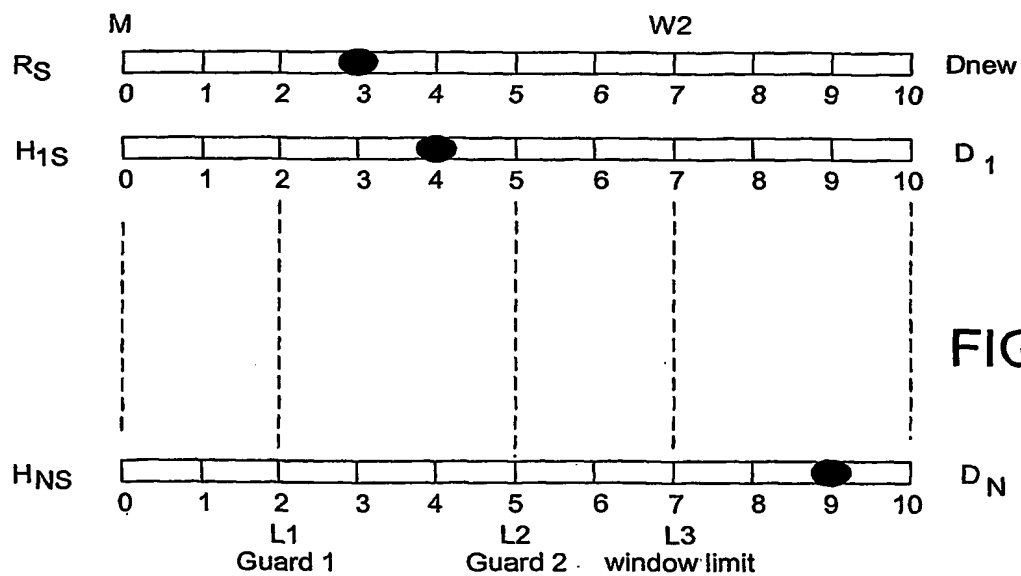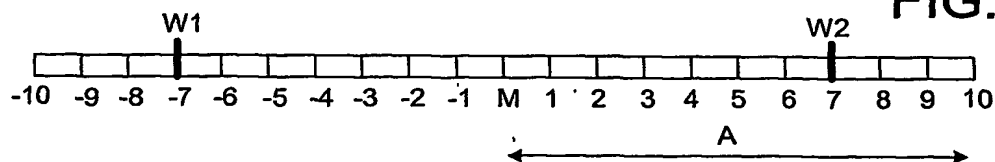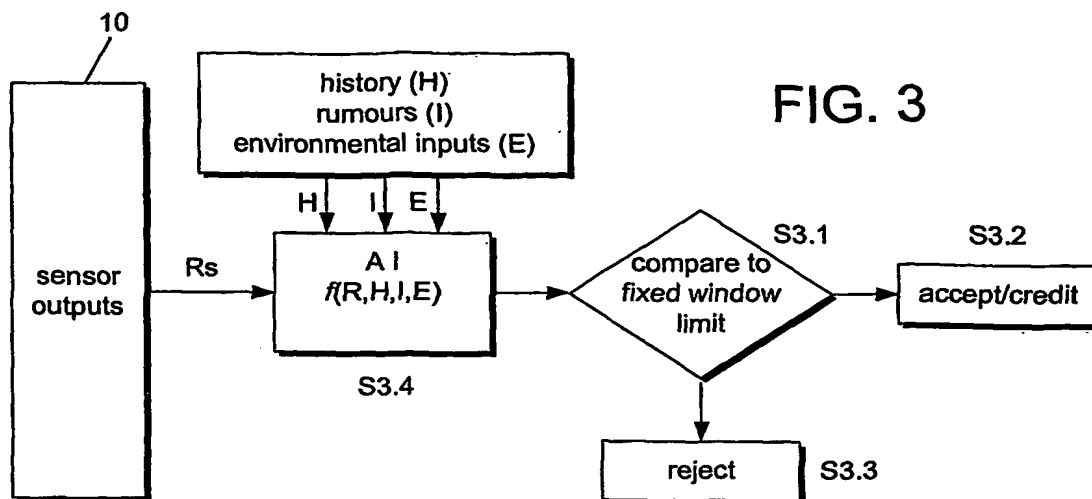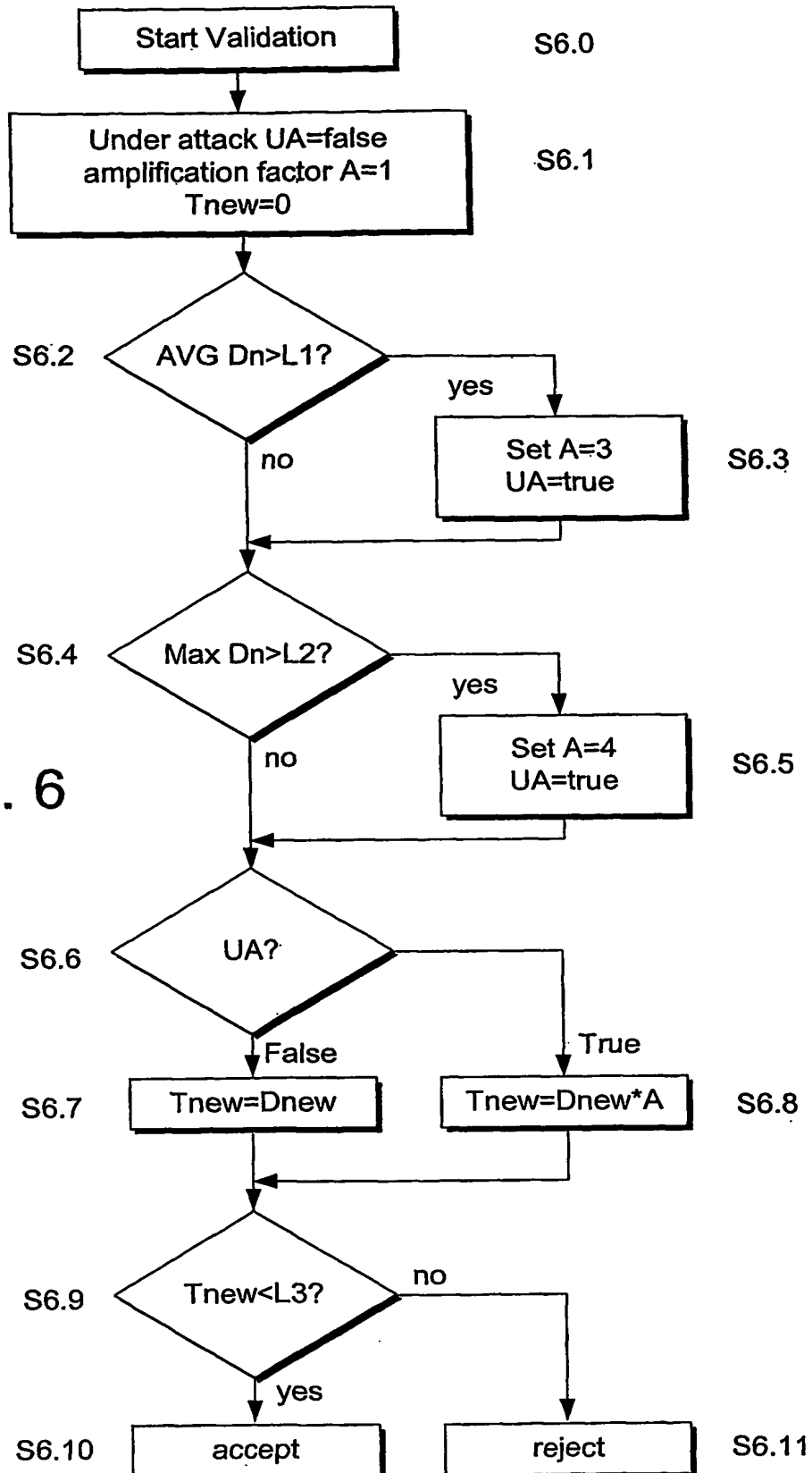**A. CLASSIFICATION OF SUBJECT MATTER**
IPC 7   G07F3/00   G07D3/00   G06N7/00   G06N5/00   G06N5/02
        G07F3/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7   G07F   G07D   G06N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 480 736 A (MARS INC) 15 April 1992 (1992-04-15) column 16, line 21 -column 20, line 16; figure 4	1-26
X	US 4 538 719 A (GRAY MATTHEW H ET AL) 3 September 1985 (1985-09-03)	1-3, 14-16, 25,26
Y	abstract; figures 1,6,13 column 15, line 40 -column 16, line 55	4-13, 17-24
Y	US 5 255 344 A (HAYASHI ISAO ET AL) 19 October 1993 (1993-10-19) abstract; figure 9 column 1, line 10 - line 13 column 5, line 28 -column 9, line 11	4-13, 17-24

-/--

X	Further documents are listed in the continuation of box C.		X	Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not
       considered to be of particular relevance
"E" earlier document but published on or after the international
       filing date
"L" document which may throw doubts on priority claim(s) or
       which is cited to establish the publication date of another
       citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or
       other means
"P" document published prior to the international filing date but
       later than the priority date claimed

"T" later document published after the international filing date
       or priority date and not in conflict with the application but
       cited to understand the principle or theory underlying the
       invention
"X" document of particular relevance; the claimed invention
       cannot be considered novel or cannot be considered to
       involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention
       cannot be considered to involve an inventive step when the
       document is combined with one or more other such docu-
       ments, such combination being obvious to a person skilled
       in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 April 2004	19/04/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Kemény, M

Form PCT/ISA/210 (second sheet) (January 2004)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BUCKLEY J J ET AL: "HYBRID NEURAL NETS CAN BE FUZZY CONTROLLERS AND FUZZY EXPERT E SYSTEMS" FUZZY SETS AND SYSTEMS, ELSEVIER SCIENCE PUBLISHERS, AMSTERDAM, NL, vol. 60, no. 2, 10 December 1993 (1993-12-10), pages 135-142, XP000405982 ISSN: 0165-0114 the whole document	1-26
A	US 2001/009485 A1 (FURUYA YONEZO) 26 July 2001 (2001-07-26) abstract; claim 7	1-26
A	US 5 355 989 A (BEST JOCHEN) 18 October 1994 (1994-10-18) abstract; figures 1,2	1-26

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0480736	A	15-04-1992	US	5167313 A	01-12-1992
			AT	137349 T	15-05-1996
			AU	662709 B2	07-09-1995
			AU	6744694 A	22-09-1994
			AU	689730 B2	02-04-1998
			AU	7407896 A	13-02-1997
			AU	678527 B2	29-05-1997
			AU	7597894 A	12-01-1995
			AU	651401 B2	21-07-1994
			AU	8947891 A	20-05-1992
			BR	9106181 A	16-03-1993
			CA	2069875 A1	11-04-1992
			CA	2194710 A1	11-04-1992
			CA	2194711 A1	11-04-1992
			DE	69119021 D1	30-05-1996
			DE	69119021 T2	28-11-1996
			DE	69133116 D1	24-10-2002
			DE	69133116 T2	16-01-2003
			EP	1156458 A2	21-11-2001
			EP	0480736 A2	15-04-1992
			EP	0685826 A2	06-12-1995
			ES	2085970 T3	16-06-1996
			ES	2181736 T3	01-03-2003
			HK	1007028 A1	26-03-1999
			IE	913594 A1	22-04-1992
			JP	7272040 A	20-10-1995
			JP	2649742 B2	03-09-1997
			JP	5502131 T	15-04-1993
			KR	9609519 B1	20-07-1996
			MX	9101534 A1	05-06-1992
			WO	9207339 A1	30-04-1992
			US	5443144 A	22-08-1995
			US	5564548 A	15-10-1996
			US	5730272 A	24-03-1998
			US	5330041 A	19-07-1994
US 4538719	A	03-09-1985	NONE		
US 5255344	A	19-10-1993	US	RE36823 E	15-08-2000
			CN	1038713 A ,B	10-01-1990
			DE	68928612 D1	23-04-1998
			DE	68928612 T2	17-09-1998
			EP	0378689 A1	25-07-1990
			EP	0813127 A2	17-12-1997
			JP	2813567 B2	22-10-1998
			JP	8320792 A	03-12-1996
			WO	8911684 A1	30-11-1989
			JP	2553725 B2	13-11-1996
			US	5168549 A	01-12-1992
US 2001009485	A1	26-07-2001	JP	10334300 A	18-12-1998
			JP	10340405 A	22-12-1998
			JP	11007565 A	12-01-1999
			JP	11031249 A	02-02-1999
			EP	0883092 A2	09-12-1998
			US	6216843 B1	17-04-2001
US 5355989	A	18-10-1994	DE	4121034 C1	10-09-1992

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US 5355989 A		DE EP ES	59207161 D1 0520230 A1 2093141 T3	24-10-1996 30-12-1992 16-12-1996